EAST TENNESSEE STATE UNIVERSITY

Acceptable Use of Information Technology Resources

Policy Effective Date: 3/24/2017 • **Policy Revised:** 6/12/2023
Procedures Effective Date: N/A • **Procedures Revised:** N/A

Policy Name: Acceptable Use of Information Technology Resources

Policy Purpose

This policy specifies the framework for the appropriate, responsible, and respectful use of University Information Technology Resources. All Users are required to act in a manner that supports the University's mission and honors the public trust. Misuse of resources can adversely affect University operations, security, and reputation.

Applicability

This policy is applicable to all users of ETSU Information Technology Resources, including students, employees, visitors, guests, and third-part vendors and contractors.

Responsible Official, Office, and Interpretation

Information Technology Services and Information Technology Council are responsible for the review and revision of this policy. For questions about this policy, please contact Information Technology Services. The Chief Information Officer, in consultation with the Office of University Counsel, has the final authority to interpret this policy.

Defined Terms

A defined term has a specific meaning within the context of this policy.

Account

A combination of credentials (such as a username and password, multifactor authentication token, or other verification method) that provides an individual with authorized access to university information technology resources.

Content

All text, images, multimedia elements, code, or other materials transmitted, stored, displayed, or processed using university information technology resources.

Data Owner

An individual with business or administrative authority over a computing system, local network, or external network connection. The Data Owner is responsible for funding,

compliance, and ensuring the system supports University objectives. Sponsorship may reside with a faculty member (e.g., research grant), department, college, or administrative unit.

Facilities Staff

Individuals authorized to monitor, manage, or provide physical access to computing or telecommunications facilities (such as computer laboratories or network rooms) used by faculty, staff, students, or the campus community.

Infrastructure Sponsor

The individual responsible for the University's information technology infrastructure and authorized to determine which information technology resources will be acquired and utilized by the University. At ETSU, this role is typically held by the Chief Information Officer (CIO).

Information Technology Resources

All computing systems, networks, electronic storage, communication, and presentation systems or services provided, owned, or operated by ETSU.

Sensitive University Data

Information that is protected against unauthorized disclosure, modification, or destruction. This includes, but is not limited to, personal information, protected health information, student education records, customer record information, cardholder data, administrative and operational plans, documents, and log data, or other confidential or legally protected information.

System Manager

An individual authorized by a Data Owner to administer, maintain, and operate a system. Responsibilities include granting, restricting, or denying User privileges, maintaining system files, communicating applicable policies to Users, and ensuring effective system operation and security. In some cases, the System Manager and Data Owner may be the same individual(s).

User

Any individual who accesses, uses, or connects to University Information Technology Resources, whether on-campus or remotely. This includes, but is not limited to, faculty, staff, students, contractors, vendors, guests, volunteers, and any other person or entity granted access to University systems, networks, or data.

Policy Name: Acceptable Use of Information Technology Resources

Policy

1. Data Owners and Operational Policies.

The University's Information Technology Resources serve a diverse community. Data Owners are responsible for establishing reasonable and appropriate requirements for the systems under their purview.

Data Owners are responsible for defining system-level priorities and operational policies, such as hours of operation, time limits, and User access. Data Owners are required to sign and conform to plan of action steps in Information Technology Services (ITS)-generated risk memos. Data Owner identity and compliance with annual cybersecurity training must be documented by ITS.

System Managers, Facilities Staff, and ITS staff are responsible for implementing and maintaining operational policies as necessary for effective system management. They are also authorized to perform routine maintenance activities, troubleshooting, system updates, and data backups, as required to ensure normal system operation.

ITS staff and authorized personnel may perform emergency maintenance on information technology systems without prior notice when needed to protect University systems, prevent data loss, mitigate security threats, or maintain service availability. Emergency maintenance may include system shutdowns, urgent updates, troubleshooting, or other necessary measures. If business processes are significantly disrupted, campus notification will be provided.

Data Owners must ensure that systems under their purview comply with all University information technology security standards, data governance requirements, and applicable laws and regulations. System Managers must implement appropriate technical and administrative controls to support compliance and safeguard University data and systems.

2. Digital Citizenship.

Digital citizenship reflects the University's expectation that all Users act with integrity, respect, and accountability when using Information Technology Resources.

2.1. User Responsibilities.

All Users of ETSU Information Technology Resources are expected to exercise responsible, lawful, and ethical behavior that upholds University policies and the public trust.

Use of ETSU Information Technology Resources must comply with all University policies, procedures, standards, and applicable laws, and must align with the University's mission.

Users must comply with all applicable state and federal laws regarding obscenity, child pornography, gambling, and gaming restrictions.

Users must not engage in conduct harms or interferes with others, including but not limited to harassment, impersonation, or disruption of legitimate Information Technology Resources.

Because acceptable use standards may vary among systems, Users are responsible for understanding and following the specific requirements of each system they access and for seeking clarification before engaging in questionable activity.

2.2. Resource Management.

ETSU Information Technology Resources must be managed and used in ways that support the University's mission and ensure fair and equitable access for all Users.

2.2.1. Priority for the use of Information Technology Resources is given to applications and activities that directly support the University's mission. Data Owners and System Managers are responsible for managing resources to ensure availability for mission-related purposes.

2.2.2. Users must not, without prior authorization, operate any device or application that consumes excessive network bandwidth or otherwise disrupts normal network operations.

2.2.3. Users must comply with all instructions from ITS staff, Facilities Staff, System Managers, Data Owners, and the Infrastructure Sponsor, including promptly vacating workstations or releasing other resources when requested.

2.3. Accessibility and Inclusivity.

Users must ensure that all digital materials created or distributed through University Information Technology Resources comply with applicable accessibility standards to support equal access for all members of the ETSU community.

3. University Rights.

ETSU reserves the right to access monitor, review, and release the Content and activity of any User Account used for University business. The university may also access:

3.1.1. Any University-owned resources;

3.1.2. Any non-University owned resources located on University property, provided documentation is submitted to and approved by the ETSU Office of University;

3.1.3. Resources connected to University networks or systems; and

3.1.4. Vendor-managed resources contracted by ETSU and containing University data.

Such actions may be taken to maintain network integrity, protect Users, safeguard infrastructure from intrusions or malicious activity, investigate suspected misuse, address security threats, or fulfill legitimate University business needs.

Access and monitoring activities will be conducted in accordance with applicable laws, University policies, and established audit and authorization procedures.

4. System and Account Privacy.

ETSU Information Technology Resources are provided for University business, educational, and research purposes. Users should have no expectation of privacy when using University computing resources, Accounts, or networks, though privacy and confidentiality are respected whenever possible in accordance with applicable laws and University policies.

4.1. Public Records.

Email, files, and other documents created, stored, or transmitted using ETSU resources may constitute public records under the Tennessee Open Records Act (T.C.A. § 10-7-501 et seq.) and may be subject to public inspection based on state law and the University's Public Records Rule, subject to statutory exemptions.

When external parties request access to University-owned or operated Information Technology Resources, including files or data, ETSU will review the request in accordance with state law and University's Public Records Rule. Information may be released only if one or more of the following conditions are met: (1) Approval by the appropriate University official(s); (2) Authorization by the owner(s) of the information; (3) Requirement by federal, state, or local law; or (4) Compliance with a valid subpoena or court order.

When disclosure is required by law, court order, or subpoena, Users will be notified as appropriate. Viewing information during normal system maintenance does not constitute disclosure. All requests from non-ETSU entities for access to University information resources will be reviewed by the ETSU Office of University Counsel before any information is released.

4.2. Monitoring and System Operations.

ETSU does not routinely monitor individual use without cause; however, system operation and maintenance require activities such as data backups, caching, activity logging, and monitoring general usage patterns.

4.3. User Responsibilities.

Users must respect the rights of others regarding privacy, intellectual property, academic freedom, freedom from harassment, and appropriate use of University resources.

Users must not intentionally seek passwords, disclose passwords, modify files or Accounts without authorization, or tamper with system restrictions or protections.

Users must preserve the privacy, dignity, and informed consent of all technology users.

4.4. Data Security and Backup.

University data may be copied to backup media periodically; the University will make reasonable efforts to maintain the confidentiality and integrity of backed-up data.

Data Owners may require investigation of systems suspected of unauthorized use, misuse, or violations of University policy or law.

Network traffic may be intercepted or analyzed as part of authorized internal or external investigations. Inbound and outbound network activity may be captured and inspected by authorities external to ETSU with or without the knowledge of ETSU.

The University complies with the Family Educational Rights and Privacy Act (FERPA) in maintaining the confidentiality of student education records.

5. System Security.

5.1. User Responsibilities.

ETSU Users are responsible for maintaining the integrity, availability, and security of University computing systems and networks, both on campus and through remote access connections and cloud services. Users must:

5.1.1. Secure physical and network access to University resources and use systems only with proper authorization;

5.1.2. Ensure hardware, software, and network components remain operational and free from unauthorized modification, damage, or disruption;

5.1.3. Avoid activities that monopolize or degrade Information Technology Resources, and ensure software installed or used supports University business or educational purposes;

5.1.4. Connect only approved network devices (e.g., switches, routers, hubs, wireless access points) with prior authorization from the Chief Information Officer (CIO) or their designee;

5.1.5. Protect University systems by keeping software applications and antivirus programs up to date and by preventing the introduction, creation, or propagation of malicious activity, including viruses, malware, spam, and phishing attempts. Exemptions for educational purposes must be approved by the CIO or their designee;

5.1.6. Refrain from actions such as IP spoofing, caller ID spoofing, email falsification, or social engineering;

5.1.7. Use only supported and patched applications and operating systems on University-owned devices, except when documented and approved by the CIO or their designee;

5.1.8. Use only University-approved cloud services to store or transmit Sensitive University Data, unless prior authorization is obtained from the CIO or their designee and the non-University service is confirmed to meet University security and compliance requirements;

5.1.9. Ensure personally owned devices used to access University systems or data comply with all applicable University security standards; and

5.1.10. Report any suspected data breach, malware infection, or other information technology security incident immediately to the ITS Help Desk.

ITS may suspend access or isolate systems to protect University Information Technology Resources and data during a suspected security incident.

6. Account Security.

6.1. User Responsibilities.

ETSU Users are responsible for safeguarding Accounts and credentials to protect University information and resources. Users must:

6.1.1. Keep all Account credentials, including passwords, PINs, tokens, or other authentication information, confidential and never share them with anyone, including friends, supervisors, ITS staff, or other employees;

6.1.2. Access only the Accounts, passwords, and privileges assigned to them, and use them solely for authorized purposes;

6.1.3. Not use University credentials to create accounts on unauthorized third-party cloud services for the storage or processing of Sensitive University Data;

6.1.4. Immediately report any unauthorized Account activity or suspected Account compromise to the ITS Help Desk and change passwords without delay;

6.1.5. Control and secure physical and network access to University resources by logging out of computers and other systems when not in use and never leaving active sessions unattended; and

6.1.6. Use multifactor authentication (MFA) when required and safeguard their authentication devices accordingly.

7. Digital Content.

Users are required to create, access, and manage digital Content in a manner that complies with applicable laws, licensing agreements, and University policies. All intellectual property and digital materials used or distributed through University Information Technology Resources must respect the rights of Content owners and uphold the University's academic and ethical standards.

7.1. Software and Licensing.

7.1.1. Software may only be copied, installed, or used on University resources as permitted by the owner and by law;

7.1.2. Users must comply with all licensing terms, including installation limits, usage restrictions, and the number of permitted users;

7.1.3. No software may be copied, shared, or distributed without confirmation that such actions are legally permissible and compliant with University policy; and

7.1.4. Users must not install software that violates the University's security policies and standards or creates a system vulnerability.

7.2. Intellectual Property and Content Use.

7.2.1. ETSU protects all legally obtained intellectual property, including copyrights, patents, trademarks, and trade secrets;

7.2.2. The presence or availability of materials on networks, including the internet, does not imply permission to use, copy, or distribute them;

7.2.3. Users must not store or transmit confidential or restricted data in violation of University data classification or storage policies; and

7.2.4. All digital Content accessed, stored, transmitted, or maintained using University resources must comply with applicable copyright laws and University policies, including the Federal Copyright Law (Title 17, U.S. Code), the Digital Millennium Copyright Act (DMCA), and the Technology, Education, and Copyright Harmonization (TEACH) Act.

7.3. Copyrights and Licenses.

Violation of copyright is prohibited under University policy and state and federal law. All copyrighted materials used through University Information Technology Resources must comply with applicable laws, University policies, and branding guidelines.

8. Compliance.

Violations of this policy may result in one or more of the following actions:

8.1.1. Immediate suspension of the User's Account, network access, or internet access, pending timely review of the charges by the appropriate authority;

8.1.2. Revocation of computing privileges at ETSU;

8.1.3. Referral to the appropriate University disciplinary process, which may include termination of employment or affiliation with ETSU, or other sanctions consistent with University policy; and

8.1.4. Referral to law enforcement for suspected violations of local, state, or federal law, which may result in civil or criminal action.

Actions taken under this policy will follow established University disciplinary procedures and provide appropriate due process protections.

Policy Name: Acceptable Use of Information Technology Resources

Procedures

N/A

Applicable Forms and Websites

Acceptable Use Policy State of Tennessee Information Technology Resources

ETSU Information Security Policy

ETSU Intellectual Property Policy

Authority and Revisions

Authority: Federal Copyright Law, Title 17 of the U.S. Code; Digital Millennium Copyright Act; Technology, Education and Copyright Harmonization Act; T.C.A. § 10-7-501 et seq; Family Educational Rights and Privacy Act

Previous Policy: N/A

The ETSU Board of Trustees is charged with policy making pursuant to TCA § 49-8-203, et seq. On March 24, 2017, the Board delegated its authority to ETSU's President to establish certain policies and procedures for educational programs and other operations of the University, including this policy. The delegation of authority and required process for revision to this policy can be found on the Policy Development and Rule Making Policy webpage.

To suggest a revision to this policy, please contact the responsible official indicated in this policy. Before a substantive change to the policy section may take effect, the requested changes must be: (1) approved by the responsible office; (2) reviewed by the Office of University Counsel for legal sufficiency; (3) posted for public comment; (4) approved by either Academic Council or University Council; and (5) approved by ETSU's President.